

Software AG

November 17, 1999
S28320US JH/Hd/mh

5

Claims

- 10 1. A method for checking the access of a user operating a first computer system controlled by a first security system to software and/or data on a second computer system controlled by a second security system comprising the following steps:
- 15 a) transmitting a user-id from said first computer system to said second computer system and a challenge from said second computer system to said first computer system,
- b) transmitting said user-id and said challenge from said first computer system to said first security system,
- 20 c) transmitting said user-id from said second computer system to a trusted agent and from said trusted agent to said second security system,
- d) transmitting a shared secret, which is registered in said first security system and in said second security system, from said second security system to said trusted agent and from said trusted agent to said second computer system,
- 25 e) calculating in said first security system a first response using said shared secret,
- f) calculating in an access control unit of said second computer system, which access control unit is able to apply the rules of the first security system to calculate a response to a challenge, a second response to said challenge using said shared secret,

- g) transmitting said first response from said first security system to said first computer system, and
- h) transmitting said first response from said first computer system to said second computer system and comparing said first response and said second response in the second computer system in order to complete the access check of said user.
2. A method according to claim 1, characterized in that the shared secret is individual to said user.
3. A method according to claim 2, characterized in that the shared secret is a hashed value of a password of said user.
4. A method according to claim 1, characterized in that the second computer system comprises a system which issues said challenge and calculates said second response according to the rules of the first security system.
5. A method according to claim 1, characterized in that the shared secret is established by the following steps:
- calculating a shared secret of a password of said user by subjecting said password to a secret function,
 - registering said shared secret in said first security system controlling said first computer system,
 - calculating an encrypted shared secret of said shared secret by subjecting said shared secret to an encryption function,
 - transmitting said encrypted shared secret to said trusted agent and further to said second security system,

-

10

15

20

25

Abstract

10. A method according to claim 1, characterized in that the communication between the first and the second computer system is done via secure channels.

11. A method according to claim 1, characterized in that the authentication of said user is effected in the first computer system and the authorisation of said user is effected in the second computer system.

12. A trusted agent for enabling the check of the access of a user operating a first computer system controlled by a first security system to software and/or data on a second computer system controlled by a second security system comprising the following functions:

- 5 a) reception of a user-id from said second computer system and transmission of said user-id to said second security system,
- b) retrieval of a shared secret, which is registered in said first security system and in said second security system, from said second security system, and
- 10 c) transmission of said shared secret from said trusted agent to said second computer system.

13. A trusted agent according to claim 12, characterized in that the first computer system is operated under Windows NT and the second computer system is operated under OS/390.

14. A computer program stored on computer readable memory means for carrying out a method according to any of the preceding method claims on a computer system.

20 15. A data carrier with a computer program for carrying out a method according to any of the preceding method claims on a computer system.

16. A method for using a computer system for carrying out a method according to any of the preceding method claims.

564221 1.634450